the system of records shall be aware of their responsibilities and are properly trained to safeguard personal information being collected and maintained under the DoD Privacy Program.

(2) Prepare promptly any required new, amended, or altered system notices for the system of records and submit them through their DoD Component Privacy POC to the DPO for publication in the FEDERAL REGISTER.

(3) Not maintain any official files on individuals which are retrieved by name or other personal identifier without first ensuring that a notice for the system of records shall have been published in the FEDERAL REGISTER. Any official who willfully maintains a system of records without meeting the publication requirements, as prescribed by 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R, is subject to possible criminal penalties and/or administrative sanctions.

§ 310.9 Privacy boards and office, composition and responsibilities.

(a) *The Defense Privacy Board*—(1) *Membership.* The Board shall consist of the DA&M, OSD, who shall serve as the Chair; the Director of the DPO, DA&M, who shall serve as the Executive Secretary and as a member; the representatives designated by the Secretaries of the Military Departments; and the following officials or their designees: the Deputy Under Secretary of Defense for Program Integration (DUSD(PI)); the Assistant Secretary of Defense for Health Affairs; the Assistant Secretary of Defense for Networks and Information Integration (ASD) (NII)/Chief Information Officer (CIO); the Director, Executive Services and Communications Directorate, WHS; the GC, DoD; and the Director for Information Technology Management Directorate (ITMD), WHS. The designees also may be the principal POC for the DoD Component for privacy matters.

(2) *Responsibilities.* (i) The Board shall have oversight responsibility for implementation of the DoD Privacy Program. It shall ensure the policies, practices, and procedures of that Program are premised on the requirements of 5 U.S.C. 552a and OMB Circular A–130, as well as other pertinent authority, and the Privacy Programs of the DoD Component are consistent with, and in furtherance of, the DoD Privacy Program.

(ii) The Board shall serve as the primary DoD policy forum for matters involving the DoD Privacy Program, meeting as necessary, to address issues of common concern so as to ensure uniform and consistent policy shall be adopted and followed by the DoD Components. The Board shall issue advisory opinions as necessary on the DoD Privacy Program so as to promote uniform and consistent application of 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R.

(iii) Perform such other duties as determined by the Chair or the Board.

(b) *The Defense Data Integrity Board*—(1) *Membership.* The Board shall consist of the DA&M, OSD, who shall serve as the Chair; the Director of the DPO, DA&M, who shall serve as the Executive Secretary; and the following officials or their designees: the representatives designated by the Secretaries of the Military Departments; the DUSD(PI); the (ASD) (NII)/CIO; the GC, DoD; the Inspector General, DoD; the ITMD, WHS; and the Director, Defense Manpower Data Center. The designees also may be the principal points of contact for the DoD Component for privacy matters.

(2) *Responsibilities.* (i) The Board shall oversee and coordinate, consistent with the requirements of 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R, all computer matching programs involving personal records contained in system of records maintained by the DoD Components.

(ii) The Board shall review and approve all computer matching agreements between the Department of Defense and the other Federal, State or local governmental agencies, as well as memoranda of understanding when the match is internal to the Department of Defense, to ensure, under 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R, appropriate procedural and due process requirements shall have been established before engaging in computer matching activities.

(c) *The Defense Privacy Board Legal Committee*—(1) *Membership.* The Committee shall consist of the Director, DPO, DA&M, who shall serve as the Chair and the Executive Secretary; the

GC, DoD, or designee; and civilian and/or military counsel from each of the DoD Components. The General Counsels (GCs) and The Judge Advocates General of the Military Departments shall determine who shall provide representation for their respective Department to the Committee. This does not preclude representation from each office. The GCs of the other DoD Components shall provide legal representation to the Committee. Other DoD civilian or military counsel may be appointed by the Executive Secretary, after coordination with the DoD Component concerned, to serve on the Committee on those occasions when specialized knowledge or expertise shall be required.

(2) *Responsibilities.* (i) The Committee shall serve as the primary legal forum for addressing and resolving all legal issues arising out of or incident to the operation of the DoD Privacy Program.

(ii) The Committee shall consider legal questions regarding the applicability of 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R and questions arising out of or as a result of other statutory and regulatory authority, to include the impact of judicial decisions, on the DoD Privacy Program. The Committee shall provide advisory opinions to the Defense Privacy Board and, on request, to the DoD Components.

(d) *The DPO*—(1) *Membership.* It shall consist of a Director and a staff. The Director also shall serve as the Executive Secretary and a member of the Defense Privacy Board; as the Executive Secretary to the Defense Data Integrity Board; and as the Chair and the Executive Secretary to the Defense Privacy Board Legal Committee.

(2) *Responsibilities.* (i) Manage activities in support of the Privacy Program oversight responsibilities of the DA&M.

(ii) Provide operational and administrative support to the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee.

(iii) Direct the day-to-day activities of the DoD Privacy Program.

(iv) Provide guidance and assistance to the DoD Components in their implementation and execution of the DoD Privacy Program.

(v) Review DoD legislative, regulatory, and other policy proposals which implicate information privacy issues relating to the Department's collection, maintenance, use, or dissemination of personal information, to include any testimony and comments having such implications under DoD Directive 5500.1.

(vi) Review proposed new, altered, and amended systems of records, to include submission of required notices for publication in the FEDERAL REGISTER and, when required, providing advance notification to the OMB and the Congress, consistent with 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R.

(vii) Review proposed DoD Component privacy rulemaking, to include submission of the rule to the Office of the Federal Register for publication and providing to the OMB and the Congress reports, consistent with 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R.

(viii) Develop, coordinate, and maintain all DoD computer matching agreements, to include the submission of required match notices for publication in the FEDERAL REGISTER and the provision of advance notification to the OMB and the Congress, consistent with 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R.

(ix) Provide advice and support to the DoD Components to ensure:

(A) All information requirements developed to collect or maintain personal data conform to DoD Privacy Program standards;

(B) Appropriate procedures and safeguards shall be developed, implemented, and maintained to protect personal information when it is stored in either a manual and/or automated system of records or transferred by electronic or non-electronic means; and

(C) Specific procedures and safeguards shall be developed and implemented when personal data is collected and maintained for research purposes.

(x) Serve as the principal POC for coordination of privacy and related matters with the OMB and other Federal, State, and local governmental agencies.

(xi) Compile and submit the ''Biennial Matching Activity Report'' to the OMB as required by OMB Circular A–

130 and DoD 5400.11–R, and the Quarterly and Annual Federal Information Security Management Agency (FISMA) Privacy Reports, as required by 44 U.S.C. 3544(c), such other reports as may be required.

(xii) Update and maintain this part and DoD 5400.11–R.

Subpart B—Systems of Records

§ 310.10 General.

(a) *System of Records.* To be subject to the provisions of this part, a ''system of records'' must:

(1) Consist of ''records'' (as defined in 310.4(r)) that are retrieved by the name of an individual or some other personal identifier; and

(2) Be under the control of a DoD Component.

(b) *Retrieval practices.* (1) Records in a group of records that MAY be retrieved by a name or personal identifier are not covered by this part even if the records contain personal data and are under control of a DoD Component. The records MUST be retrieved by name or other personal identifier to become a system of records for the purpose of this part.

(i) When records are contained in an automated (Information Technology) system that is capable of being manipulated to retrieve information about an individual, this does not automatically transform the system into a system of records as defined in this part.

(ii) In determining whether an automated system is a system of records that is subject to this part, retrieval policies and practices shall be evaluated. If DoD Component policy is to retrieve personal information by the name or other unique personal identifier, it is a system of records. If DoD Component policy prohibits retrieval by name or other identifier, but the actual practice of the Component is to retrieve information by name or identifier, even if done infrequently, it is a system of records.

(2) If records are retrieved by name or personal identifier, a system notice must be submitted in accordance with § 310.33.

(3) If records are not retrieved by name or personal identifier but then are rearranged in such a manner that they are retrieved by name or personal identifier, a new systems notice must be submitted in accordance with § 310.33.

(4) If records in a system of records are rearranged so that retrieval is no longer by name or other personal identifier, the records are no longer subject to this part and the system notice for the records shall be deleted in accordance with § 310.34.

(c) *Relevance and necessity.* Information or records about an individual shall only be maintained in a system of records that is relevant and necessary to accomplish a DoD Component purpose required by a Federal statute or an Executive Order.

(d) *Authority to establish systems of records.* Identify the specific statute or the Executive Order that authorizes maintaining personal information in each system of records. The existence of a statute or Executive Order mandating the maintenance of a system of records does not abrogate the responsibility to ensure that the information in the system of records is relevant and necessary. If a statute or Executive Order does not expressly direct the creation of a system of records, but the establishment of a system of records is necessary in order to discharge the requirements of the statute or Executive Order, the statute or Executive Order shall be cited as authority.

(e) *Exercise of First Amendment rights.* (1) Do not maintain any records describing how an individual exercises his or her rights guaranteed by the First Amendment of the U.S. Constitution except when:

(i) Expressly authorized by Federal statute;

(ii) Expressly authorized by the individual; or

(iii) Maintenance of the information is pertinent to and within the scope of an authorized law enforcement activity.

(2) First Amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.